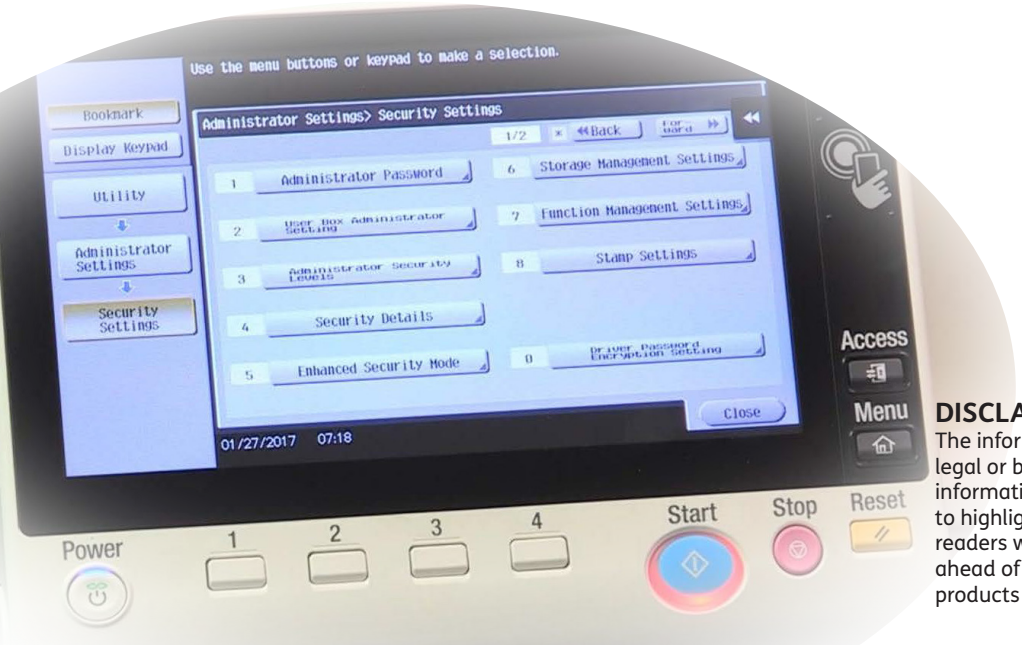
Olivetti

Preparing for GDPR

INTRODUCTION

There are many aspects of Multifunctional Devices (MFPs), Document Workflow Solutions and Printers that meet the stringent criteria for data security and, in this overview document, we will identify some of these areas to help readers to conduct their own assessments. More details can be obtained from Olivetti Dealers and Olivett's Technical Support Team.

CONTENTS:



DISCLAIMER:
The information within this document does not constitute legal or binding advice. It is simply an overview of practical information, gleaned from the IOC and other relevant sources, to highlight as many facts as possible, which could assist readers with preparations for their own businesses and systems ahead of the new regulations and to explain how Olivetti products comply with GDPR. E&OE.

The GDPR is Europe's new framework for Data Protection laws replacing the previous 1995 Data Protection Act, which current UK law is based upon.

What is the GDPR?

The General Data Protection Regulation (GDPR) is a legally binding act of legislation, which comes into force on the 25th May 2018, issued by the European Union to enhance personal data protection throughout Europe. It builds on and reaches beyond the existing Data Protection Acts of each European country and will unify the law under the new regulations.

The fact that the UK is planning to leave the European Union makes no difference – the regulations still apply as there will still be contact and business conducted with companies and individuals throughout the UK and Europe.

The new regulations have been brought about because it has been argued that the current laws have proved to be inconsistent over the years and they seek to make everyone who collects, handles, stores or manages personal data, responsible for safe-guarding the data and that those who fail to comply with the new regulations are made accountable for their actions.

Quick Glance Summary

WHEN DOES THE NEW REGULATION START?

May 25th 2018

WHO WILL ENFORCE IT IN THE UK?

The Information Commissioner's Office

WHAT'S NEW?

There are new rights for people to have access to the information companies hold about them, rules for better data management for businesses, and a new tough regime of fines.

WHAT ABOUT BREXIT?

The UK is implementing a new Data Protection Bill which includes provisions of the GDPR. There are some small changes but our own law will be largely the same.

The regulations will carry heavy penalties for those who fail to comply. Fines of up to 20 million € or 4% of a company's global turnover (whichever is higher) can be enforced, which is not only financially devastating but carries with it the stigma of long-term damage to the company's reputation.

"We live in a world where cyber attacks are a fact of life." - *Business Reporter - The Telegraph*

Why has GDPR become necessary?

Currently, each EU Member State has their own Data Protection Policy and the UK is working to the 1995 Data Protection Act (**DPA**).

What this doesn't do is take into account the rate of technological evolution, making some of the current legislation largely obscelete now. Therefore, the GDPR aims to unify all the Member States under one set of regulations and it has been designed to be "future-proof" to allow for further rapid changes in technology and any business advancements by companies in the EU or who use EU data.

Another aspect of the DPA in the UK is that it is seen as having some inconsistencies with other countries' policies and that can leave individuals vulnerable when data is shared between Member States, as they all have different levels of protection. With Cyber Attacks becoming more of an issue, data protection is vital for businesses and individuals. At the moment, it's very difficult for individuals to find out who has their data and what they are doing with it. The new GDPR will put paid to that level of worry.

With data being produced at exponential rates, world-wide, and being used as a commercial commodity by unscrupulous companies, hackers, scammers etc, the dangers for everyone are increased.

Breaches of privacy are often an after-thought at the design stage of product manufacturing so reports of vulnerabilities and inefficient security repairs, along with product recalls are on the rise.

"If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them."

- Henry David Thoreau, Author (1817 -1862)

Greater Rights for Individuals

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

"The first level of vulnerability is an organic one - people." - *Stephen Hawking*

"There's a lot in the GDPR you'll recognise from the current law, but make no mistake, this one's a game changer for everyone. "

Elizabeth Denham - IOC Commissioner

What are the Key Principles of the new regulations?

1. Who does GDPR apply to?

The GDPR applies to **'Controllers'** and **'Processors'** of data. The Controller says how and why personal data is processed and the Processor acts on the Controller's behalf.

The GDPR places specific legal obligations on a Processor. For example, Processors are required to maintain records of personal data and processing activities. They will have significantly more legal liability if they are responsible for a breach. These obligations for Processors are a new requirement under the GDPR.

However, a Controller is not relieved of their obligations where a Processor is involved – the GDPR places further obligations on a Controller to ensure their contracts with Processors comply with the GDPR.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including data processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal or household activities.

What data does GDPR apply to?

(i) Personal Data

Like the current DPA, the GDPR applies to 'Personal Data'. However, the GDPR's definition is "any information relating to an identified or identifiable natural person" and makes it clear that even information, such as an online identifier, such as an IP address, or location information can be personal data.

Under GDPR there is a wide range of 'personal identifiers' which constitutes personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists or contact details etc, should make little practical difference if information is held that falls within the scope of the current DPA, as it will also fall within the remit of the GDPR.

"Attack where they are unprepared, appear where you are not expected." - *Sun Tzu, The Art of War c. 544-496 BC*

"The most significant addition is the Accountability Principle; to show HOW Processors and Controllers comply with the principle." *IOC*

What data does GDPR apply to?

(i) Personal Data continued.../

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This goes beyond the scope of the current DPA's definition and could include sets of manual records containing personal data which is ordered chronologically.

If personal data has been coded with a nick-name or pseudonym then it can still fall within the bounds of the GDPR depending on how difficult it is to attribute the nick-name or pseudonym to a particular individual.

(ii) Sensitive Personal Data

Sensitive Personal Data according to the GDPR is referred to as "special categories of personal data" including: data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

These categories are similar to the current DPA but with the addition of genetic data and biometric data which has been processed to identify a specific individual. Personal data relating to criminal convictions and offences are not included, but extra safeguards apply to how it's collected, handled and processed.

Article 5 of the GDPR requires that Personal and Sensitive Personal Data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

> **"The biggest mistake any hardware user can make is to ignore backing up their data. "**
>
> *CyberSmart.org*

Technology and GDPR

The GDPR consists of 8 Main Principles that cover all aspects of the regulations, all of which are explained, in detail, in the document, produced by the IOC, called "***Guide to Data Protection***". The 7th Principle is one that can be related to technology involved in the handling and management of data, which involves printers and document management tools. It states that "**appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**".

In practice, it means companies and individuals must have appropriate security to prevent the personal data held from being accidentally or deliberately compromised. In particular, companies will need to:

- **Design and organise their security** to fit the nature of the personal data they hold and the harm that may result from a security breach;
- **Be clear about who, in their organisation, is responsible** for ensuring information security;
- **Make sure they have the right physical and technical security**, backed up by robust policies and procedures and reliable, well-trained staff; and
- **Be ready to respond** to any breach of security swiftly and effectively.

Advances in technology have enabled organisations to process more and more personal data, and to share information more easily. This has obvious benefits if they are collecting and sharing personal data in accordance with the Data Protection Principles, but it also gives rise to equally obvious security risks.

The more databases that are set up and the more information that is exchanged, the greater the risk that the information will be lost, corrupted or mis-used.

A number of high-profile losses of large amounts of personal data, in recent years, have brought attention to the issue of information security. The IOC's ***"Guide to Data Protection"*** document gives examples of possible breaches, in each area, and explains who would be responsible and accountable for these in a live situation.

However, these incidents have also made it clear that information security is an issue of public concern as well as technical compliance. If personal data is not properly secured, this can seriously damage an organisation's reputation and future and can also compromise the safety of individuals.

"A password is like underwear: you don't let people see it, you should change it very often, and you shouldn't share it with strangers."

Chris Pirillo - founder and CEO of LockerGnome, Inc

Security through MFP Devices and Document Solutions

Multifunctional devices (MFP) such as printers and scanners are often overlooked when it comes to data security. They attach to a company's network and enable users to scan to email and the cloud. They can also store a degree of personal data, such as email and IP addresses and can also save jobs in their sophistocated memories to enable people to print at a later stage.

There are many web-based document software solutions, which link to MFP products for the purpose of scanning documents, that enables companies to integrate paper-based workflows, inbound emails and faxes to document management systems, databases, corporate file servers and content management applications. It's a form of data capture so, by their very nature, are the responsibility of Data Processors and Data Controllers. However, in the case of some products, such as those that don't actually store data on them - ie they push the storage to a number of other devices, whether they be the Cloud or other digital storage devices - they are not holding information after the data has been processed.

What can you do to check you comply?

There are so many things to assess but there is still plenty of time to do so. By setting out your stall to carry out a full and far-reaching assessment over the next few months, there is time to be thorough, leave no stone unturned and prevent breaches in your security.

Firstly, advice being given by official sources is to use a Checklist and carry out a Risk Assessment on your company's activities surrounding data capture, handling, processing, storage systems and how information is shared and printed and what happens to printed documents and how and where they are filed.

It is also wise to put in place an assured strategy and even a contingency plan for how to deal with a breach - in the unlikely event that would happen. Once a through strategy is in place it's possible to make sure printers, MFPs and document management solutions have been set up with the latest security kits, authentication structures and encryption facilities.

> **"Safety and security don't just happen, they are the result of collective consensus and public investment ."**
>
> *Nelson Mandella*

How are our products compliant with GDPR?

Under the 7th Principle of the GDPR, today's printers and MFPs should be treated no differently than any other IT peripheral connected to the network as they use hard drives, processors and network cards found in any PC.

At Olivetti our printers, MFPs and Document Management software have been developed to protect users from unauthorised access and leaks of information through a network, via mobile devices, by the copying, interference or deletion of information or through equipment failure, accidental loss or damage by a user or job logs being accessed.

All our latest MFPs achieve the Compatible Criteria Certification (ISO/IEC 15408) as well as the IEEE 2600.1 Security Standard either through standard security features that are built into the machines when they are manufactured or as a result of adding optional data security kits.

As this is a very far-reaching topic, we will cover a few of the basic aspects of how our machines are security ready. For more details please contact our Technical Team.

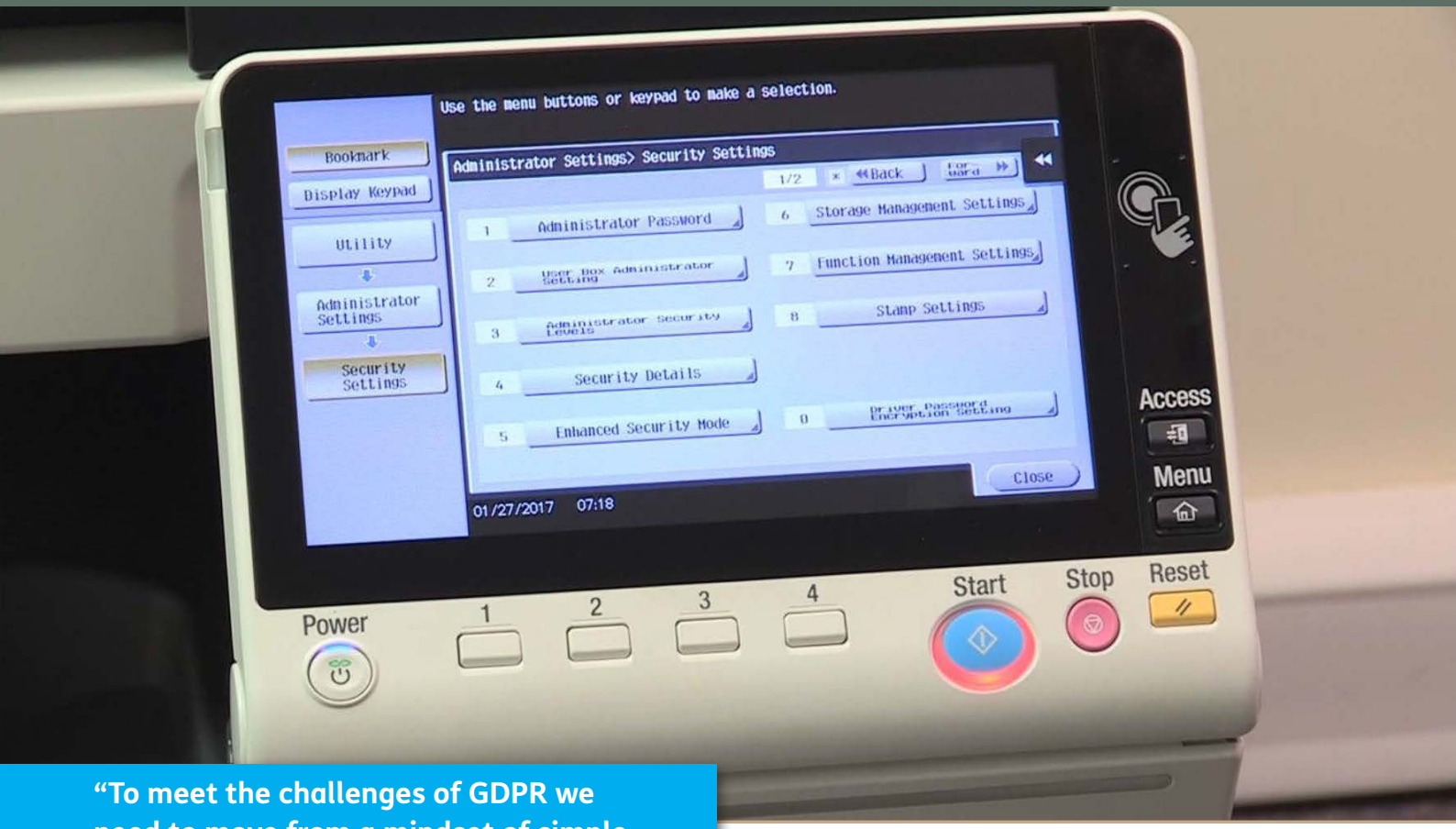
1. Security for image and output processing

When data is scanned in via the MFP's scanner, it is processed, compressed and written to the MFP's memory. To print this data it is decompressed and sent to the printer, where it is output to paper. However, after the print has been completed the compressed data is deleted from the memory and the image data in the memory is overwritten, page by page, so it cannot be printed out or transferred again.

It is possible for job data to be stored on the hard drive (HDD), in the form of unique compressed data but even if this internal data could be read, analysing it would be virtually impossible. What is more, on most MFP models, the HDD itself can be encrypted as standard. It is also possible to lock the HDD password which would further prevent unauthorised access.

By using the secure print feature, a print job can be saved temporarily on the MFP's memory, so that a user can collect it later but only after inputting a PIN, password or using a personal ID card or a biometric trigger to access the print file.

"Of the most common pieces of security advice, given by experts, users will follow some diligently while ignoring others, depending on their own mental models of security. " - *Robert W. Reeder, Google*



"To meet the challenges of GDPR we need to move from a mindset of simple compliance to a mindset of commitment to managing data sensitively and ethically, because it's part of basic good business practice." *Elizabeth Denham - IOC*

2. User authentication

To enable the measurement of use, restriction of usage and, more importantly, the prevention of mis-use, MFPs support user authentication and can set permission rules for individuals, registered addresses or departments to have restricted access to important features from colour printing, duplex output, scanning to emails, access to box data to the setting of an upper limit for output sheet data, or using the fax. There are various forms of user accessed authentication from a personal password, PIN, ID Card or biometric trigger, such as finger-vein recognition, for each individual in a company.

3. Protecting Data on the Hard Drive (HDD)

As mentioned, previously, internal data on the HDD can be overwritten to delete the data on there. This is done by overwriting with random numbers through the MFP's settings. As well as this, the HDD can be locked, and only accessible with a password, so even if the HDD is removed from the machine and attached to a PC, it cannot be accessed. All data on the HDD can be encrypted with an Advanced Encryption Standard (AES) and a built-in encryption module (OpenSSL/MES) and cannot be read or decrypted without an Encryption Key.

The activity of the MFP is saved as an Audit Log. This can trace any unauthorised access but it is simply a record for reporting only and cannot be accessed to print or transfer previous tasks or data.

4. The Encryption of PDF Files

Data scanned with the MFP and saved in PDF format can be encrypted with a common key or code. To open an encrypted PDF file, using Adobe Acrobat, the common key or code must be entered.

5. Protecting e-mail Data

When a user sends an e-mail through the MFP, they can register to the recipient's address book, using a code, to encrypt the e-mail, and then the receiver can use their own private key or code to decrypt the e-mail they receive on their PC. This allows for secure sending and receiving, without the content of the e-mail being intercepted by others. The sender also can add a signature to an e-mail with the MFP key, which the receiver has to verify with the MFP Certificate, using a TPM chip. This allows the receiver to confirm that the email was not intercepted.

"Over the course of March, 2016 – March, 2017, we identified 788,000 potential victims of keylogging; 12.4 million potential victims of phishing; and 1.9 billion usernames and passwords exposed by data breaches. "

Survey by Google & International Computer Science Institute

6. Scan to Me, Scan to Home and Scan to Authorised Folder

An individual is able to scan data to themselves by configuring the MFP's user authentication. A "Me" button and a "Home" button are displayed in the registered address column, by enabling the feature in Administrator settings.

If "Me" was selected for the address, it is sent to the e-mail address of the authenticated user, and if "Home" was selected, it is sent to the PC folder registered, in advance, allowing for sending files quickly with one touch.

SMB authentication can be restricted to SMB addresses other than the individual's by leaving the [user ID] and [password] columns of the SMB address empty. If a logged-in user selects their own SMB address from the address book and presses 'send', then the authenticated user-name and password are used without change.

By restricting and prohibiting the direct input of addresses through the Administrator settings, it can be set up so that only the Administrator can manage the send destinations, taking away the potential for mis-use and the sending of data to unauthorised email addresses.

7. Dealing with viruses

The intergrated controller on our colour MFPs uses a Linux kernel integrated into the MFP and most viruses, are more likely to attack Windows based Operating Systems, due to the nature that they are more open and tend to allow viruses an easier way in.

In most cases, USB memory viruses are run and cause infection simply by being inserted. However, because there is no mechanism in an MFP for a run file to be opened, due to the Linux based kernel, viruses held on a USB device have no effect.

There are features on an MFP allowing for the connection to a USB device, which allows (i) the printing of image data from a USB device (ii) saving scanned image data and (iii) image data saved to the Box to the USB device, but these features have to be activated by the user, so they will not run automatically and it could be easy to trace the perpetrator.

Furthermore, the USB interface path and network path are separated based on system architecture. Even if an MFP is connected by USB to a PC connected to the Internet, the MFP cannot be accessed from the Internet environment through the PC.

Further Reading

The following White Papers and Guidance Documents are available on-line at:
www. ico.org.uk

Consultation: GDPR consent guidance
ICO - Information Commissioner's Office

Overview of the General Data Protection Regulation (GDPR)
ICO - Information Commissioner's Office

Preparing for the General Data Protection Regulation (GDPR)
ICO - Information Commissioner's Office

IOC Preparing for the GDPR 12 Steps
ICO - Information Commissioner's Office V2.0 20170525

Guide to Data Protection
ICO - Information Commissioner's Office

Direct Marketing Guidance
ICO - Information Commissioner's Office

Direct Marketing Checklist
ICO - Information Commissioner's Office

www.olivetti.com